

Federal Communications Commission 445 12th Street, S.W. Washington, D. C. 20554

News Media Information 202 / 418-0500 Internet: http://www.fcc.gov TTY: 1-888-835-5322

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC. 515 F 2d 385 (D.C. Circ 1974).

FOR IMMEDIATE RELEASE:

July 3, 2014

FCC NEWS MEDIA CONTACT:

Mike Snyder, 202-418-0997 Email: michael.snyder@fcc.gov

MPDC NEWS MEDIA CONTACT:

Gwendolyn Crump, 202-727-9346 Email: gwendolyn.crump@dc.gov

CONSUMER ADVISORY

TIPS FOR PROTECTING YOUR MOBILE DEVICE FROM THEFT

As you celebrate the Fourth of July, remember to be "smart" about your smartphone

Washington, D.C. – As the Independence Day holiday weekend approaches, D.C. Metropolitan Police Chief Cathy Lanier and FCC Consumer and Governmental Affairs Acting Bureau Chief Kris Monteith today issued a list of tips to raise consumer awareness about protecting mobile devices from theft.

Record device information. Mobile devices have unique numbers (IMEI or MEID numbers) that can identify devices if they are stolen. You should record the IMEI or MEID number, serial number and MAC/Wi-Fi address and store it in a safe place. This information is usually found under the "Settings" menu on the "About" screen. Additionally, screenshot functions make it easy to capture this information and send it to an email account. **Before you go out**:

- Find the IMEI or MEID number on your mobile device
- Send yourself a screenshot of it: <u>iOS (Apple)</u>, <u>Android</u>, <u>Blackberry</u>, and <u>Windows</u>

Be aware of your surroundings. Many mobile device thefts are crimes of opportunity. Using your device in public, particularly on public transit, or leaving it out in the open makes it easier for thieves to grab the device and run.

Treat mobile device theft like credit card theft. Mobile devices frequently contain sensitive financial and personal information.

Report all mobile device thefts immediately to your wireless carrier and local law enforcement.

Set a password/PIN and use the lock screen function. The password/PIN and lock screen functions on devices make it more difficult for thieves to use your stolen device and access your personal data. These functions should be set up as soon as you purchase a new device. (CTIA The Wireless Association has instructions for setting up a password on Android, Blackberry, Apple and Windows devices.)

Consider using mobile security apps. Mobile security apps can be useful in locating and recovering stolen devices. Common features include the ability to remotely track, lock or erase your personal data on your mobile devices. Some apps also allow you to remotely trigger an alarm on the device or take a photo of the thief. CTIA provides a list of mobile security apps.

Regularly back up photos and data. Photos, videos, contacts, email and other data you would want to keep if your device is stolen should backed up regularly on a computer, USB drive or cloud service.

Locate, lock and erase. You should inform law enforcement of your mobile security app that might help locate and recover the device. In addition, the remote lock feature can prevent thieves from using your stolen device. It may be best to remotely erase your personal data on the device if you believe it will not likely be recovered or if it contains sensitive financial, health or work information.

For More Information

Visit http://www.fcc.gov/guides/stolen-and-lost-wireless-devices and http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data for more information about protecting your mobile devices. A Spanish-language version of these consumer tips is also available.

-FCC-

Safety and Crime Prevention information is available from MPDC at http://mpdc.dc.gov/page/safety-and-crime-prevention

News and other information about the FCC is available at www.fcc.gov